

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2002-152271
 (43) Date of publication of application : 24. 05. 2002

(51) Int. Cl. H04L 12/56
 G06F 17/30
 H04L 12/28

(21) Application number : 2001-109398 (71) Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>
 (22) Date of filing : 09. 04. 2001 (72) Inventor : KOMIYA TERUYUKI
 FUJI HITOSHI

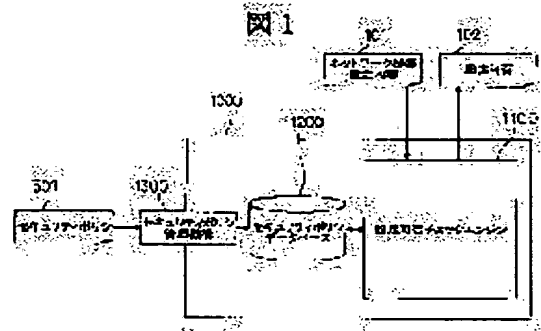
(30) Priority
 Priority number : 2000265058 Priority date : 01. 09. 2000 Priority country : JP

(54) SECURITY POLICY HIGH-SPEED RETRIEVAL METHOD, DEVICE AND RECORDING MEDIUM RECORDED WITH PROGRAM THEREFOR

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a security policy high-speed retrieval method and device that can suppress increasing rate of a retrieval time, with respect to the increase in setting items and the increase in an entry registered as a security policy.

SOLUTION: The security policy high-speed retrieval method and device has a security policy storage procedure, that stores security policy possessed by a network manager to a computer system and a setting propriety check procedure, that checks the propriety of setting request for a network device, on the basis of the security policy.



LEGAL STATUS

[Date of request for examination]
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

Copyright (C) ; 1998, 2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2002-152271

(P2002-152271A)

(43)公開日 平成14年 5月24日 (2002.5.24)

(51)Int.Cl. ⁷	識別記号	F I	テ-マコ-ト*(参考)
H 0 4 L 12/56		H 0 4 L 12/56	Z 5 B 0 7 5
G 0 6 F 17/30	1 7 0	G 0 6 F 17/30	1 7 0 Z 5 K 0 3 0
H 0 4 L 12/28	2 0 0	H 0 4 L 12/28	2 0 0 Z 5 K 0 3 3

審査請求 未請求 請求項の数13 O L (全 10 頁)

(21)出願番号 特願2001-109398(P2001-109398)
(22)出願日 平成13年4月9日(2001.4.9)
(31)優先権主張番号 特願2000-265058(P2000-265058)
(32)優先日 平成12年9月1日(2000.9.1)
(33)優先権主張国 日本 (J P)

(71)出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72)発明者 小宮 輝之
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内
(72)発明者 富士 仁
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内
(74)代理人 100083552
弁理士 秋田 収喜

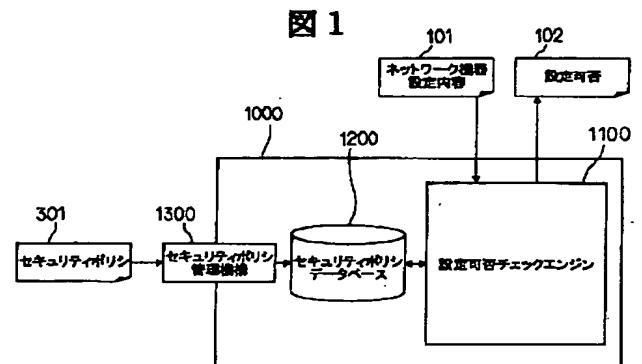
最終頁に続く

(54)【発明の名称】 セキュリティポリシ高速検索方法、装置及びそのプログラムを記録した記録媒体

(57)【要約】

【課題】 設定を行う項目の増加やセキュリティポリシとして登録されるエントリの増加に対して、検索時間の増加率を抑える。

【解決手段】 ネットワーク管理者が保持しているセキュリティポリシをコンピュータシステムに保持するセキュリティポリシ保持手順と、ネットワーク機器の設定要求をセキュリティポリシによって設定の可否をチェックする設定可否チェック手順とを有することを特徴とするセキュリティポリシ高速検索方法および装置。



【特許請求の範囲】

【請求項 1】 ネットワーク管理者が保持しているセキュリティポリシーをコンピュータシステムに保持するセキュリティポリシー保持手順と、ネットワーク機器の設定要求をセキュリティポリシーによって設定の可否をチェックする設定可否チェック手順とを有することを特徴とするセキュリティポリシー高速検索方法。

【請求項 2】 前記セキュリティポリシーは、一つの機器の設定に必要な項目の組に対して、許可された設定内容をあてはめたものを一単位とし、この単位ごとに一意な識別子が付与されることを特徴とする請求項 1 に記載のセキュリティポリシー高速検索方法。

【請求項 3】 前記セキュリティポリシー保持手順は、パケットフィルタリングにおけるソース側 IP アドレス範囲とデスティネーション側 IP アドレス範囲のように二つの設定値範囲として扱えるものは、一つの設定項目として扱い、それぞれを x 軸、y 軸上にマッピングした平面図形として表現し、セキュリティポリシーとして登録されたエントリの数を N としたときに、与えられた長方形が、すでに存在する長方形と部分的に重なる、または含まれるかどうかを判断する処理時間のオーダーが $O(N)$ 以下となるデータ構造を用いることを特徴とする請求項 1 に記載のセキュリティポリシー高速検索方法。

【請求項 4】 前記設定可否チェック手順は、2 次元データ検索を行う 2 次元データ検索手順と、検索対象を管理する検索対象管理手順とからなることを特徴とする請求項 1 乃至 3 のうちいずれか 1 項に記載のセキュリティポリシー高速検索方法。

【請求項 5】 前記 2 次元データ検索手順は、前記のセキュリティポリシーのデータ構造を用いて、前記判断に対する処理時間が、セキュリティポリシーとして登録されたエントリの数を N としたときの処理時間のオーダー $O(N)$ 以下の処理時間で検索処理を行うことを特徴とする請求項 4 に記載のセキュリティポリシー高速検索方法。

【請求項 6】 前記検索対象管理手順は、セキュリティポリシーの中で検索対象となるエントリの識別子を管理する手順であり、複数の設定項目に対して検索処理を行う際に、他の項目の検索結果から、検索が不要と判断されるエントリの識別子を検索対象から取り除くことを特徴とする請求項 4 又は 5 に記載のセキュリティポリシー高速検索方法。

【請求項 7】 ネットワーク管理者が保持しているセキュリティポリシーをコンピュータシステムに保持するセキュリティポリシー保持手段と、ネットワーク機器の設定要求をセキュリティポリシーによって設定の可否をチェックする設定可否チェック手段とを有することを特徴とするセキュリティポリシー高速検索装置。

【請求項 8】 前記セキュリティポリシーは、一つの機器の設定に必要な項目の組に対して、許可された設定内容

をあてはめたものを一単位とし、この単位ごとに一意な識別子が付与される手段であることを特徴とする請求項 7 に記載のセキュリティポリシー高速検索装置。

【請求項 9】 前記セキュリティポリシー保持手段は、パケットフィルタリングにおけるソース側 IP アドレス範囲とデスティネーション側 IP アドレス範囲のように二つの設定値範囲として扱えるものは、一つの設定項目として扱い、それぞれを x 軸、y 軸上にマッピングした平面図形として表現し、セキュリティポリシーとして登録されたエントリの数を N としたときに、与えられた長方形が、すでに存在する長方形と部分的に重なる、または含まれるかどうかを判断する処理時間のオーダーが $O(N)$ 以下となるデータ構造であることを特徴とする請求項 7 に記載のセキュリティポリシー高速検索装置。

【請求項 10】 前記設定可否チェック手段は、2 次元データ検索を行う 2 次元データ検索手段と、検索対象を管理する検索対象管理手段とからなることを特徴とする請求項 7 乃至 9 のうちいずれか 1 項に記載のセキュリティポリシー高速検索装置。

【請求項 11】 前記 2 次元データ検索手段は、前記のセキュリティポリシーのデータ構造を用いて、前記判断に対する処理時間が、セキュリティポリシーとして登録されたエントリの数を N としたときの処理時間のオーダー $O(N)$ 以下の処理時間で検索処理を行う手段であることを特徴とする請求項 10 に記載のセキュリティポリシー高速検索装置。

【請求項 12】 前記検索対象管理手段は、セキュリティポリシーの中で検索対象となるエントリの識別子を管理する手段であり、複数の設定項目に対して検索処理を行う際に、他の項目の検索結果から、検索が不要と判断されるエントリの識別子を検索対象から取り除く手段であることを特徴とする請求項 10 又は 11 に記載のセキュリティポリシー高速検索装置。

【請求項 13】 請求項 1 乃至請求項 6 のいずれか 1 項に記載のセキュリティポリシー高速検索方法の処理手順を、コンピュータに実行させるためのプログラムを記録したコンピュータ読み出し可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、仮想閉域網 (VPN: Virtual Private Network) 製品などのネットワーク機器を利用して、ネットワークを介して通信を行うことによって作られる論理閉域網に関し、特に、前もって定めたセキュリティポリシーに基づいてネットワーク機器の設定内容の設定可否をチェックする際に、高速にチェックを行う方法及び装置に関する。

【0002】

【従来の技術】ネットワーク上に、物理的なネットワーク構成に依存しない論理閉域網を構成するには、パケットフィルタリング (以下、P. F. と称する) や VPN

3

等いくつかのネットワーク機器を設定する。ネットワーク管理者は、各ネットワーク機器の、IP (Internet Protocol) アドレスやポート番号など設定すべき複数の項目全てに関して、設定内容がネットワークの属する組織の方針であるセキュリティポリシーの範囲内であるかどうかを調べ、設定を許可するかどうかを判断する。このとき、ネットワーク管理者は、設定内容がセキュリティポリシーの範囲内かをチェックするために、複数の項目ごとに、事前に登録されたセキュリティポリシーのうち該当する項目のエントリ全体に対して検索を行う。

【0003】

【発明が解決しようとする課題】前記従来の技術では、設定内容がセキュリティポリシーの範囲内かをチェックするための検索時間は、設定を行う項目の増加、及びセキュリティポリシーとして登録されるエントリの増加に比例して長くなる。ネットワークが大規模化することは、一般に、設定を行うネットワーク機器の増加やセキュリティポリシーとして登録するエントリの増加が伴うため、従来の技術では困難になる。また、きめ細かいセキュリティポリシーを定義することも、セキュリティポリシーとして登録するエントリの増加が伴うため、従来の技術では困難になる。本発明は、前記従来技術の問題点を解決するためになされたものであり、本発明の目的は、設定を行う項目の増加やセキュリティポリシーとして登録されるエントリの増加に対して、検索時間の増加率を抑えることが可能な技術を提供することにある。本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

【0004】

【課題を解決するための手段】本願において開示される発明の概要を簡単に説明すれば、下記のとおりである。ここでいう、ネットワーク利用者とは、通信を行うコンピュータなどをネットワークに接続し、そのコンピュータを使用する人物であり、ネットワーク機器とは、コンピュータが通信を行うネットワークに接続されている機器やソフトウェアである。また、ネットワーク管理者とは、ネットワーク利用者が利用できるコンピュータやサービスの決定など、ネットワーク機器の管理方針を作成し、ネットワーク機器の設定を行う人物である。また、論理閉域網とは、ゲートウェアやファイアウォールなどで物理的に他のネットワークと切り離されている物理ネットワークに制限されることなく、特定のコンピュータなどだけが通信できるように、情報に特定の識別子を付与したり、特定の鍵による暗号化を施すことによって実現するネットワークである。

【0005】本発明は、ネットワーク管理者が保持しているセキュリティポリシーをコンピュータシステムに保持しておくセキュリティポリシー保持手段と、ネットワーク機器の設定要求をセキュリティポリシーによって設定の可否をチェックする設定可否チェック手段とからなるセキ

4

ュリティポリシー高速検索方法及び装置である。前記セキュリティポリシー保持手段では、セキュリティポリシーは、一つの機器の設定に必要な項目の組に対して、許可された設定内容をあてはめたものを一単位とし、この単位ごとに一意な識別子が付与される。

【0006】さらに、P. F. におけるソース (source) 側 IP アドレス範囲とデスティネーション (destination) 側 IP アドレス範囲のように二つの設定値範囲として扱えるものは、一つの設定項目として扱い、それぞれを x 軸、y 軸上にマッピングした平面図形として表現し、ウィンドウ質問 (与えられた長方形が、すでに存在する長方形と部分的に重なる、または含まれるかどうかを判断することを、一般にウィンドウ質問と呼ぶ) に対する処理時間が $O(N)$ 以下となるデータ構造を用いる。ここで、 $O(N)$ は、セキュリティポリシーとして登録されたエントリの数を N としたときの処理時間のオーダーを表し、 N が増加するときに、処理時間が一次関数で増加することを意味する。ウィンドウ質問に対する処理時間が $O(N)$ 以下となるデータ構造として、領域 4 分木や MX-CIF 4 分木、R 木などが挙げられる。

【0007】前記設定可否チェック手段は、2次元データ検索を行う 2次元データ検索手段と検索対象を管理する検索対象管理手段からなり、この二つの手段によって高速な検索を実現する。前記 2次元データ検索手段は、前記のセキュリティポリシーのデータ構造を用いて O

(N) 以下の処理時間で検索処理を行う手段である。前記検索対象管理手段は、セキュリティポリシーの中で検索対象となるエントリの識別子を管理する手段であり、複数の設定項目に対して検索処理を行う際に、他の項目の検索結果から、検索が不要と判断されるエントリの識別子を検索対象から取り除くことで、全てのエントリに対して検索を行う場合よりも高速な検索を実現する。また、前記セキュリティポリシー保持手段におけるデータ構造が、2次元データ検索を行う前にあらかじめ一部の検索対象を除外することが困難なデータ構造の場合であっても、一般に、セキュリティポリシーのチェックにあたる平面図形同士の比較よりも、識別子の比較の処理時間の方が小さいため、より高速な検索が実現できる。

【0008】ネットワーク管理者は、セキュリティポリシーをコンピュータシステムにデータとして保存しておく。ここでのコンピュータシステムを、以下では、セキュリティポリシー検索装置と呼び、データをセキュリティポリシーデータベースと呼ぶ。ネットワーク管理者が、ネットワーク利用者から要求された論理閉域網の構成条件をもとに導出したネットワーク機器の設定要求をセキュリティポリシー検索装置に入力すると、セキュリティポリシー検索装置は、セキュリティポリシーで許可されている範囲かをチェックし、設定の可否を出力する。

【0009】

【発明の実施の形態】以下、図面を参照して本発明の実

施の形態を詳細に説明する。なお、実施の形態を説明するための全図において、同一機能を有するものは同一符号を付け、その繰り返しの説明は省略する。図1は、本発明による一実施形態（実施例）のセキュリティポリシー検索装置の概略構成を示す模式図である。図1において、1000はセキュリティポリシー検索装置、101はネットワーク機器設定内容、102はネットワーク機器設定内容101に対する設定可否、301はセキュリティポリシー、1100はネットワーク管理者からのネットワーク機器設定内容101を受付けて設定可否102を導出する設定可否チェックエンジン、1200はセキュリティポリシー301を保存するセキュリティポリシーデータベース、1300はネットワーク管理者からのセキュリティポリシー301を受付けてセキュリティポリシーデータベース1200を更新するセキュリティポリシー管理機構である。

【0010】図1に示すように、本実施形態（実施例）のセキュリティポリシー検索装置1000は、ネットワーク管理者からのネットワーク機器設定内容101を受付けて設定可否102を導出する設定可否チェックエンジン1100と、セキュリティポリシー301を保存するセキュリティポリシーデータベース1200とで構成される。前記セキュリティポリシー301について、P.F.におけるソース側IPアドレス範囲とデスティネーション側IPアドレス範囲、ソース側ポート範囲とデスティネーション側ポート範囲、アドレス変換におけるプライベート（private）側IPアドレス範囲とグローバル（global）側IPアドレス範囲、VPNにおけるソース側IPアドレス範囲とデスティネーション側IPアドレス範囲、及びソース側ポート範囲とデスティネーション側ポート範囲は、二つの設定値範囲を一組として扱い、それぞれをx軸、y軸上にマッピングした平面図形として表現する。

【0011】前記P.F.、及びVPNにおけるソース側IPアドレス範囲とデスティネーション側IPアドレス範囲“(src_ip.from~src_ip.to)→(dst_ip.from~dst_ip.to)”は、src_ip.from~src_ip.to間の任意のIPアドレスをソース側アドレスとし、ds

t_ip.from~dst_ip.to間の任意のIPアドレスをデスティネーション側アドレスとするIPアドレス対を指す。一つのIPアドレス対は、2次元平面上の、一つの長方形として表現される（図2）。ただし、src_ip.from≤src_ip.to、及びdst_ip.from≤dst_ip.toの条件が成り立っているとする。

【0012】前記P.F.、及びVPNにおけるソース側ポート範囲とデスティネーション側ポート範囲“(src_port.from~src_port.to)→(dst_port.from~dst_port.to)”は、src_port.from~src_port.to間の任意のポートをソース側ポートとし、dst_port.from~dst_port.to間の任意のポートをデスティネーション側ポートとするポート対を指す。一つのポート対は、2次元平面上の、一つの長方形として表現される。ただし、src_port.from≤src_port.to、及びdst_port.from≤dst_port.toの条件が成り立っているとする。

【0013】アドレス変換におけるプライベート（private）側IPアドレス範囲とグローバル（global）側IPアドレス範囲“(private_ip.from~private_ip.to)→(global_ip.from~global_ip.to)”は、private_ip.from~private_ip.to間のIPアドレス（プライベート側）から、global_ip.from~global_ip.to間のIPアドレス（グローバル側）への対応を定義したアドレス変換対を指す。一つのアドレス変換対は、表1に示すようにアドレス変換の種類（名称はRFC2663“IP Network Address Translator (NAT) Terminology and Considerations”の定義による）によって、2次元平面上で図3に示す図形として表現される。ただし、private_ip.from≤private_ip.to、及びglobal_ip.from≤global_ip.toの条件が成り立っているとする。

【0014】

【表1】

アドレス変換の種類と図形の形状

アドレス変換の種類		図形の形状
Two-Way NAT	Static NAT	線分(private_ip.from, global_ip.from)-(private_ip.to, global_ip.to) ただし、private_ip.to-private_ip.from=global_ip.to-global_ip.from
	Basic NAT	線分(private_ip.from, global_ip.from)-(private_ip.to, global_ip.to) ただし、private_ip.to-private_ip.from=global_ip.to-global_ip.from
Traditional NAT	NAPT	線分(private_ip.from, global_ip.from)-(private_ip.to, global_ip.to) ただし、global_ip.from=global_ip.to

ネットワーク機器設定内容101について、P.F.やアドレス変換、VPNに関するネットワーク機器設定内容は、セキュリティポリシー301と同様、二つの設定値

範囲を一組として扱い、それぞれをx軸、y軸上にマッピングした平面図形として表現する。

【0015】図4は、セキュリティポリシー検索装置10

00の状態遷移を示す図であり、図5は、前記セキュリティポリシ検索装置1000の処理手順を示すフローチャートである。前記セキュリティポリシ検索装置1000の処理手順は、図5に示すように、まず、初期状態において、ネットワーク管理者が、セキュリティポリシ301を定め、セキュリティポリシ管理機構1300からセキュリティポリシ検索装置1000へ入力することで、セキュリティポリシデータベース1200へ新規追加を行う（ステップ201）。

【0016】この状態以降は、ステップ202での処理内容の判定に基づき、ネットワーク管理者が、セキュリティポリシ301を定め、セキュリティポリシ管理機構1300からセキュリティポリシ検索装置1000へ入力することによる、セキュリティポリシデータベース1200の更新処理（ステップ203）、及びネットワーク管理者が、ネットワーク機器設定内容101を定め、設定可否チェックエンジン1100へ入力することによる、設定可否102の導出処理（ステップ204）が任意に行われる。また、ステップ203での更新処理の後に、セキュリティポリシデータベース1200が空か否かを判断し（ステップ205）、セキュリティポリシデータベース1200が空の場合、即ち、ネットワーク管理者が、セキュリティポリシ管理機構1300からセキュリティポリシ検索装置1000へ指示することで、セキュリティポリシデータベース1200を全て削除した場合には初期状態に戻り、セキュリティポリシ検索装置1000は、ネットワーク機器設定内容101を受付けることはできなくなる。

【0017】図6は、前記設定可否チェックエンジン1100の処理手順を示すフローチャートである。前記設定可否チェックエンジン1100の処理手順は、図6に示すように、まず、前記設定可否チェックエンジン1100は、ネットワーク管理者からネットワーク機器設定内容101の入力を受付ける（ステップ211）。次に、入力されたネットワーク機器設定内容101の種類が判断され（ステップ212）、ステップ212での判断結果に基づき、入力されたネットワーク機器設定内容101の種類に対応した設定可否チェックを行い（ステップ213～ステップ215）、設定可否102を求める。そして、設定可否チェックエンジン1100は、設定可否102の内容をネットワーク管理者へ返す（ステップ216）。

【0018】図7は、前記設定可否チェックエンジン1100で行われる設定可否チェックの処理手順を示すフローチャートである。前記設定可否チェックの処理は、図7に示すように、設定可否チェックエンジン1100に入力されたネットワーク機器設定内容101を設定要求Rとし、Rがセキュリティポリシデータベース1200で管理されているセキュリティポリシPによって許可されているかのチェックを行い、その結果を設定可否1

02として出力する。また、設定不可の場合には、“設定不可”と、設定許可と判断された設定値のリストと、設定不可と判断された設定値のリストを出力する。ネットワーク管理者は、受取った設定可否結果102が設定可であった場合、一般には入力したネットワーク機器の設定内容101の設定を行う。また、受取った設定可否結果102が設定不可であった場合、ネットワーク管理者は、入力したネットワーク機器の設定内容101のうち設定可と判断された部分だけの設定を行う、もしくはネットワーク機器の設定内容101を破棄する。

【0019】前記設定可否チェックの処理手順は、図7に示すように、初めに、ネットワーク機器設定内容101の設定要求Rが入力されると（ステップ221）、 $j=1$ とし（ステップ222）、次に、対象リストの初期値として、1からnの値を設定するとともに不可リストを空集合とする（ステップ223）。ここで、対象リストは、セキュリティポリシPのうち、検索対象となる P_i を指す識別子 i の集合である。セキュリティポリシPとして登録されたエンタリは、必ずしも一つではなく、複数存在する場合もある（数1の式）。なお、この P_i において、 i が本発明の識別子に相当する。ここで、設定要求 $R = \{RC1, RC2, \dots, RCj, \dots, RCm\}$ 、セキュリティポリシ $P_i = \{Ci1, Ci2, \dots, Cij, \dots, Cim\}$ とし、 RCj と Cij はIPアドレスやポート番号などの設定項目である。

【0020】

【数1】

$$(P = \sum_{i=1}^n P_i)$$

そこで、対象リストに識別子が含まれる Cj （数2の式）から RCj の平面検索を行い（ステップ225）、 $RCj(x) \wedge \neg Cj(x)$ となる x が存在するか否かを判断し（ステップ226）、ステップ226でNoの場合は、ステップ228に進み、ステップ226でYesの場合には、許可されない設定値の項目をその許可されない値で置き換えたRを、不可リストへ加える（ステップ227）。次に、 RCj と部分的に重なる、又は、 RCj を含む Cij を指す識別子 i のみを対象リストに残す（ステップ228）。前述のステップ225からステップ228までのセキュリティによるチェック処理は、ステップ224と、ステップ229及びステップ230により、Rの各項目 RCj （ $j=1, 2, \dots, m$ ）全てについて調べる。

【0021】Rの全項目が調べ終わった時点で、不可リストが空集合か否かを判断し（ステップ231）、ステップ231で、不可リストが空集合のままの場合には、全ての RCj がセキュリティポリシによって許可されたと判断し、“設定可”を出力する（ステップ234）。ステップ231で、不可リストが空集合ではない場合に

は、Rから不可リストの設定値を取り除いたものを許可リストとし（ステップ232）、"設定不可"、許可リスト、不可リストを出力する（ステップ233）。ステップ225での、RCjの設定値が、セキュリティポリシの一部分であるCj（数2の式）によって許可されて

$$C_j = \sum_{i=1}^n c_{ij}$$

図形RCj上にある全ての点xが、図形集合Cjに含まれる図形の少なくとも一つの図形Cijと重なっていれば、図形RCjで表現される設定要求は、セキュリティポリシによって設定することが許可されていると判断する。これは、数3の式の真偽値を判定することと等しい。RCj(x) ∧ ¬Cj(x) となるxが存在しなければ真、つまり図形Rで表現される設定要求はセキュリティポリシによって設定することが許可されていると判断する。この処理を行うためには、まず、RCjと部分的に重なる、またはRCjを含むCijを検索する必要がある。この検索は、前述のようにCijのデータ構造として領域4分木などのデータ構造を用いることで、C1jからCnjまでのそれぞれとRCjとを比較した場合よりも高速に行うことが可能である。

【0023】

【数3】 $\forall x (RC_j(x) \rightarrow C_j(x)) \equiv \neg \exists x \neg (RC_j(x) \rightarrow C_j(x)) \equiv \neg \exists x \neg (\neg RC_j(x) \vee C_j(x)) \equiv \neg \exists x (RC_j(x) \wedge \neg C_j(x))$

RCj(x) ∧ ¬Cj(x) が存在しない：RCjが意味する設定要求は設定可能

RCj(x) ∧ ¬Cj(x) が存在する：RCjが意味する設定要求は設定不可

（数3の式のセキュリティポリシによる設定可否チェック）

RC1に関するセキュリティポリシのチェックの検索対象は、C11からCn1の全てとし、RC(j+1)に関するセキュリティポリシのチェックの検索対象は、RCjに関するセキュリティポリシのチェックの検索において、RCjと部分的に重なる、又はRCjを含むCijのiに相当するCi(j+1)のみとする。jが増加するにつれて検索対象が絞られるため、RCjのそれぞれにおいてC1jからCnjの全てを対象として検索を行う場合よりも高速に検索を行うことが可能である。前記設定要求RCjとセキュリティポリシCijの関係を図8に示す。

【0024】図9は、前記セキュリティポリシ管理機構1300の処理手順を示すフローチャートである。前記セキュリティポリシ管理機構1300は、ネットワーク管理者からセキュリティポリシ301の入力を受付け（ステップ241）、受付けたセキュリティポリシ301の処理内容を判断し（ステップ242）、その処理内容をもとにセキュリティポリシデータベース1200の

いるかどうかの判断は、RCjの表す図形が、Cjが表す図形集合に含まれるかを調べることで実現する。

【0022】

【数2】

削除（ステップ243）、更新（ステップ244）、あるいは追加（ステップ245）を行う。なお、前記各処理は、コンピュータ上で動作するコンピュータプログラムによっても実現可能であり、前記各処理を実行するコンピュータプログラムは、コンピュータが読み取り可能な記録媒体で提供される。ここで、コンピュータ読み取り可能な記録媒体とは、フロッピー（登録商標）ディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記録装置をいう。以上、本発明者によってなされた発明を、前記実施の形態に基づき具体的に説明したが、本発明は、前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【0025】

【発明の効果】本願において開示される発明によって得られる効果を簡単に説明すれば、下記のとおりである。本発明によれば、ネットワーク機器の設定内容が、セキュリティポリシによって許可されているかを高速に検索する手段を設けたので、設定を行う項目の増加やセキュリティポリシとして登録されるエントリの増加に対して、検索時間の増加率を抑えることができる。これにより、ネットワークを大規模化や、きめ細かいセキュリティポリシの定義を行うことができる。

【図面の簡単な説明】

【図1】本発明による一実施形態（実施例）のセキュリティポリシ検索装置の概略構成を示す模式構成図である。

【図2】本実施形態のIPアドレス対の表現を示す図である。

【図3】本実施形態のアドレス変換対の表現を示す図である。

【図4】本実施形態のセキュリティポリシ検索装置の状態遷移図である。

【図5】本実施形態のセキュリティポリシ検索装置の処理手順を示すフローチャートである。

【図6】本実施形態の設定可否チェックエンジンの処理手順を示すフローチャートである。

【図7】本実施形態の設定可否チェック処理手順を示すフローチャートである。

【図8】本実施形態の設定要求とセキュリティポリシの関係を示す図である。

11

【図 9】本実施形態のセキュリティポリシー管理機構のセキュリティポリシーによる設定可否チェック処理手順を示すフローチャートである。

【符号の説明】

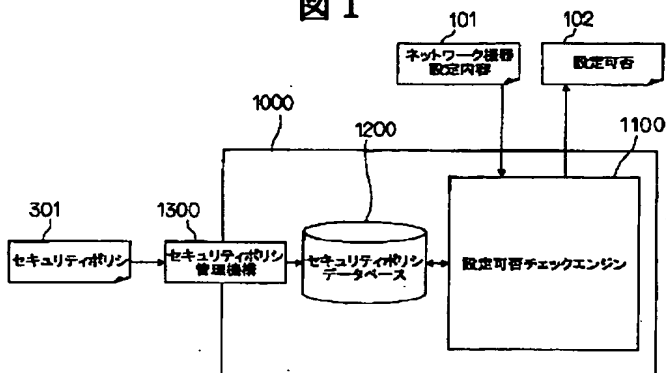
1000…セキュリティポリシー検索装置、1100…設

12

定可否チェックエンジン、1200…セキュリティポリシーデータベース、1300…セキュリティポリシー管理機構、101…ネットワーク機器設定内容、102…設定可否、301…セキュリティポリシー。

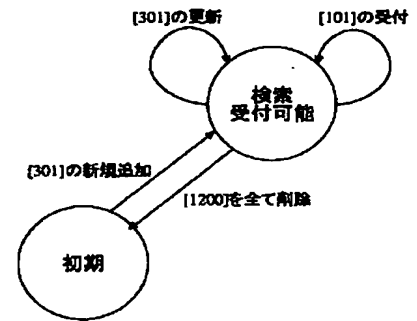
【図 1】

図 1



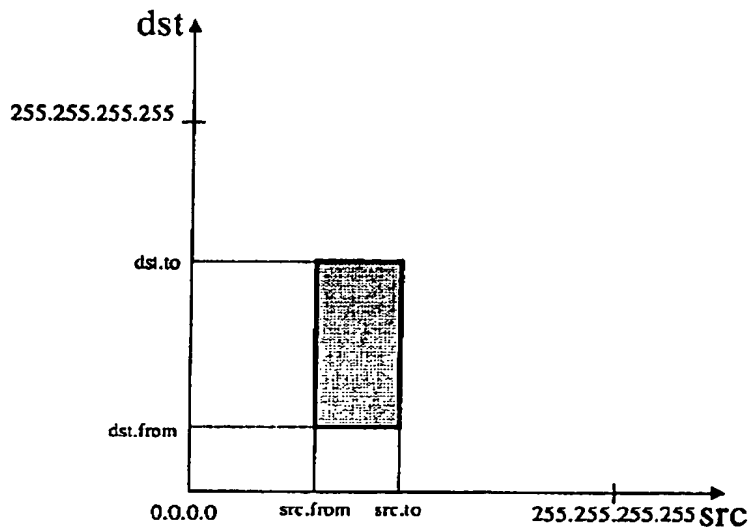
【図 4】

図 4



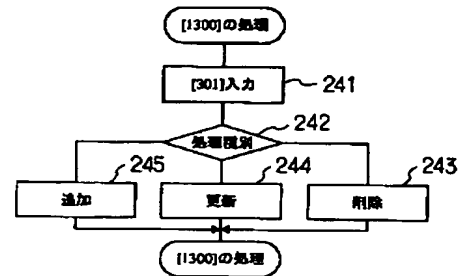
【図 2】

図 2



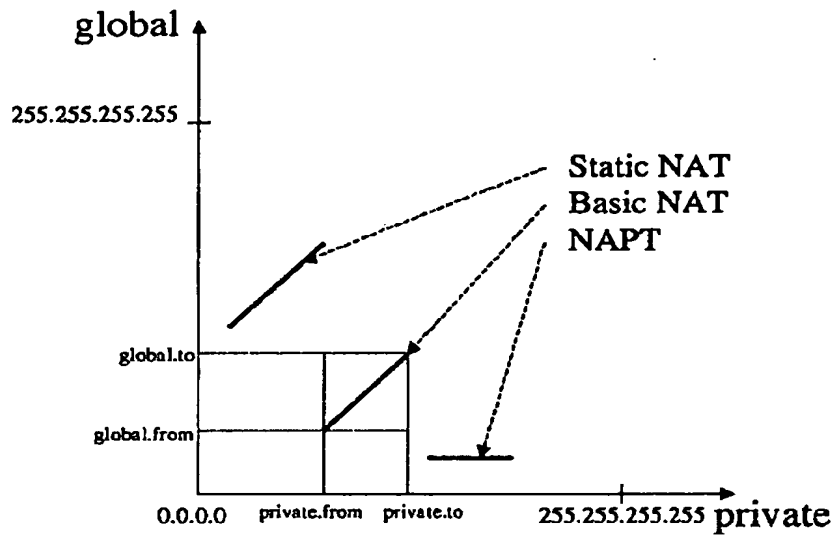
【図 9】

図 9



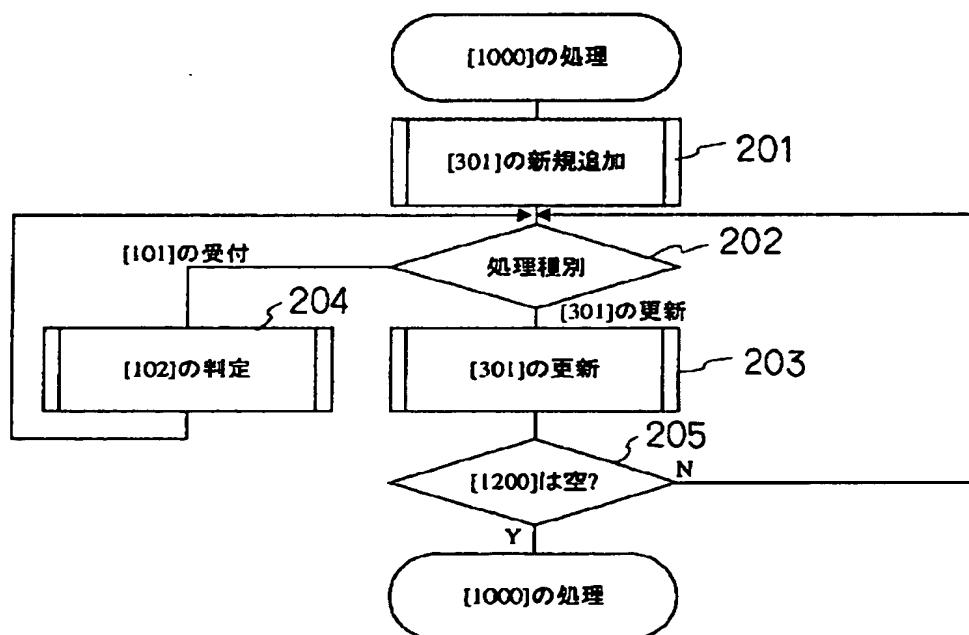
【図 3】

図 3



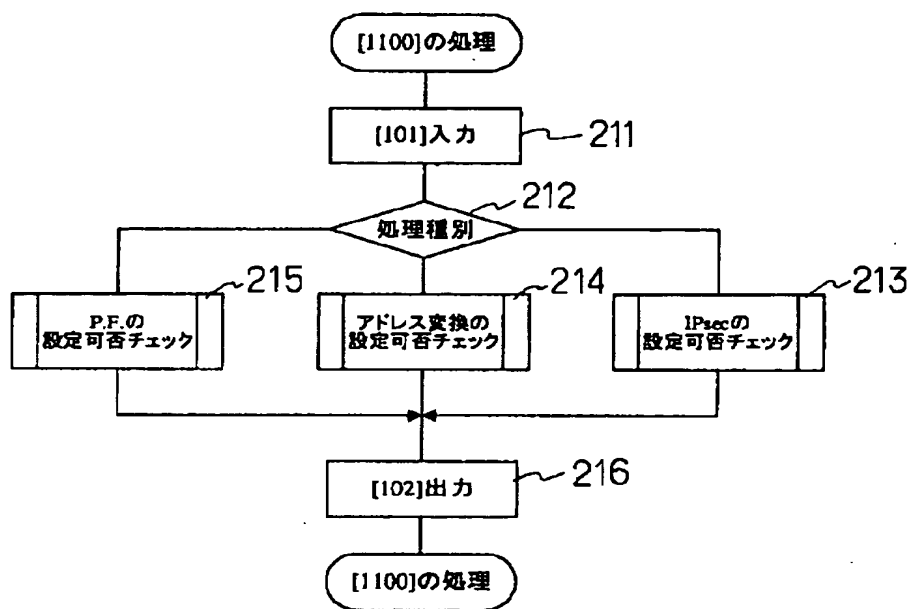
【図 5】

図 5



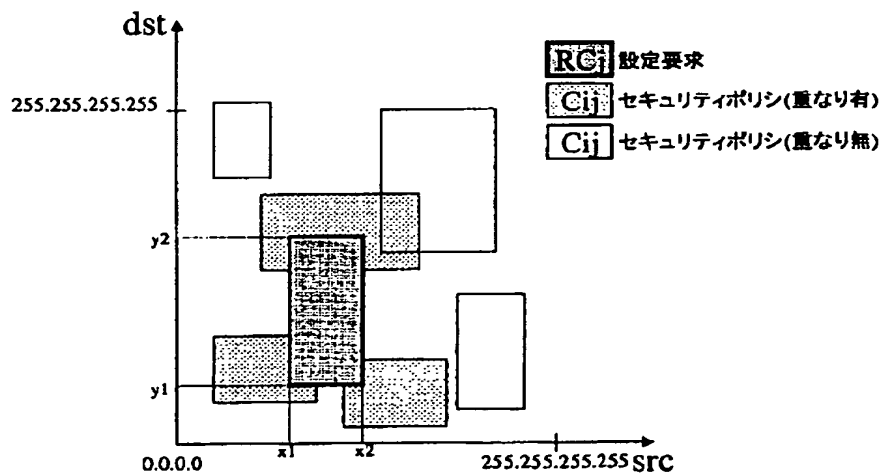
【図6】

図 6



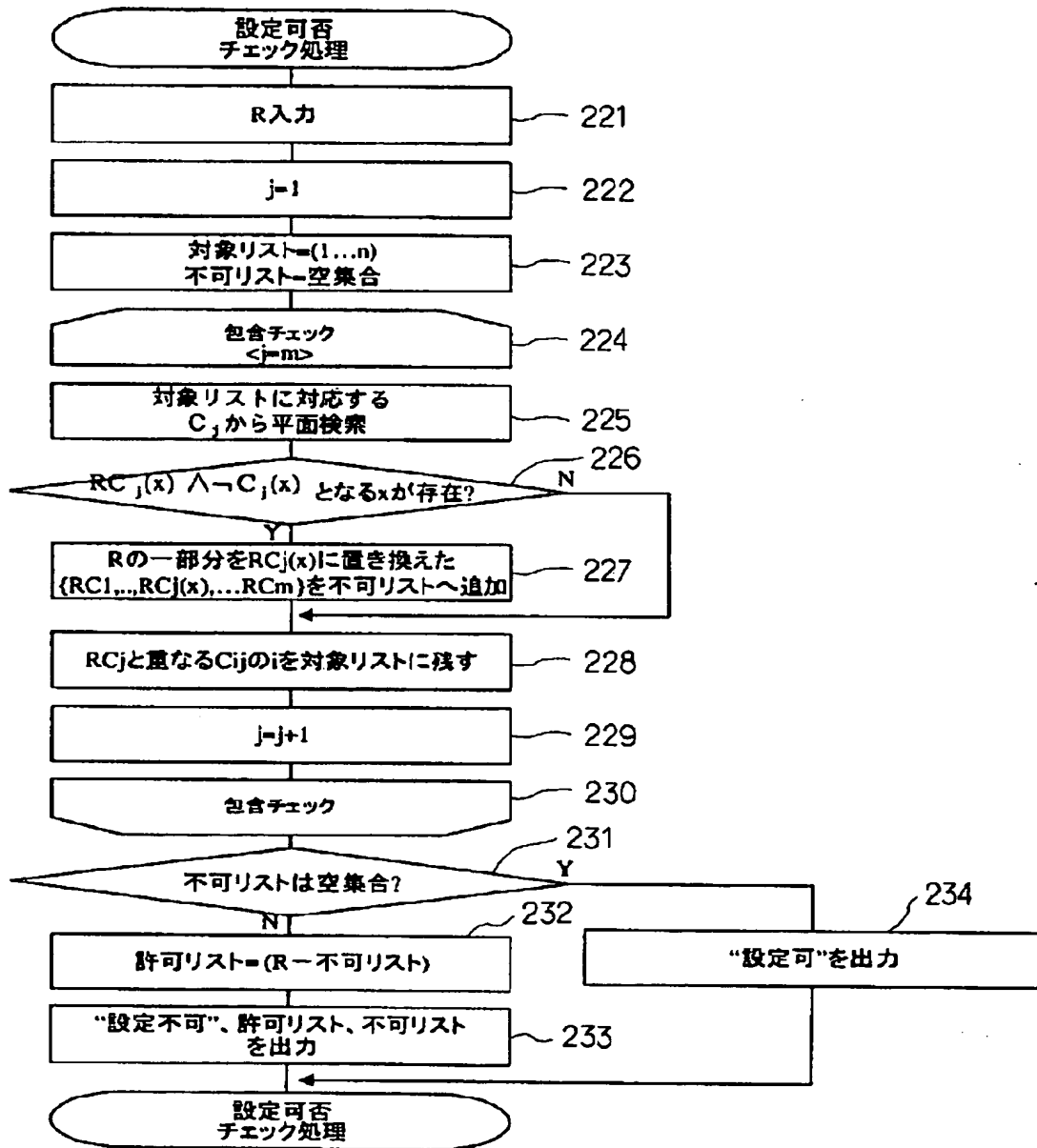
【図8】

図 8



【図 7】

図 7



フロントページの続き

F ターム (参考) 5B075 KK02 KK43 KK70 UU40
 5K030 GA15 HA08 HB08 HB19 HD09
 KA07 LB05 LC13 LD17
 5K033 AA08 BA08 CB09 CC01 DB12
 DB14